PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ^{6} **:** **H04L 9/32**	**A1**	**(11) International Publication Number:** **WO 96/33568** **(43) International Publication Date:** 24 October 1996 (24.10.96)

(21) International Application Number: PCT/GB96/00915

(22) International Filing Date: 17 April 1996 (17.04.96)

(30) Priority Data:
9507885.3 18 April 1995 (18.04.95) GB

(71) Applicant *(for all designated States except US)*: HEWLETT-PACKARD COMPANY [US/US]; 3000 Hanover Street, Palo Alto, CA 94304 (US).

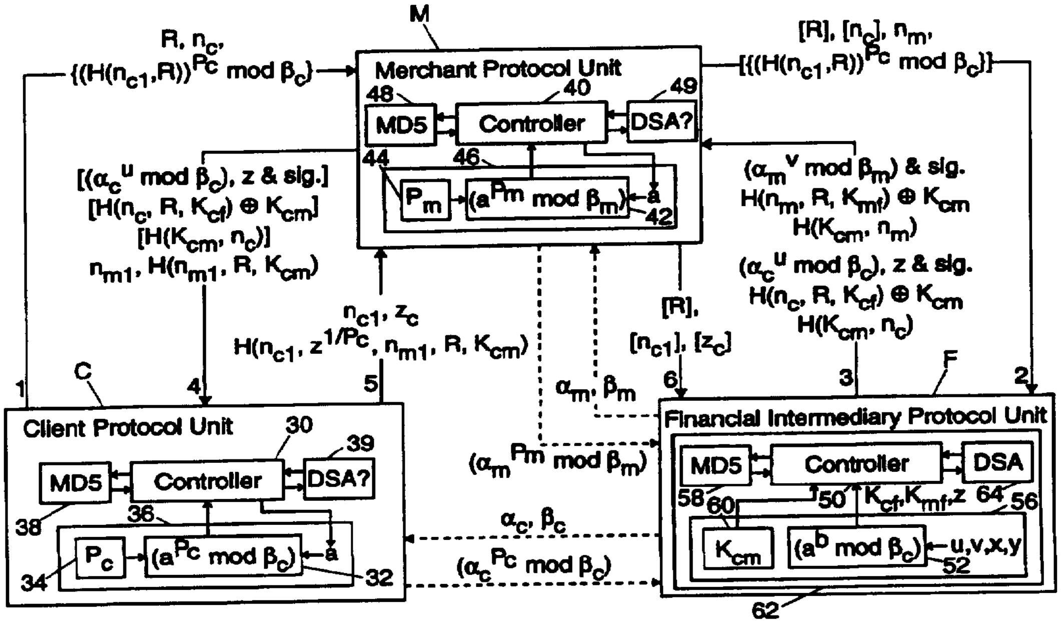
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: MAO, Wenbo [CN/GB]; 60 Wheatfield Drive, Bradley Stoke, Bristol BS12 9DD (GB).

(74) Agent: COKER, David, Graeme; Hewlett-Packard Limited, Intellectual Property Section, Building 2, Filton Road, Stoke Gifford, Bristol BS12 6QZ (GB).

(81) Designated States: JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHODS AND APPARATUS FOR AUTHENTICATING AN ORIGINATOR OF A MESSAGE


M
$R, n_c,$
$\{(H(n_{c1},R))^{Pc} \bmod \beta_c\}$
Merchant Protocol Unit
48
40
49
MD5
Controller
DSA?
44
46
P_m
$(a^{Pm} \bmod \beta_m)$
a
42
$[R], [n_c], n_m,$
$[\{(H(n_{c1},R))^{Pc} \bmod \beta_c\}]$
$[(\alpha_c{}^u \bmod \beta_c), z$ & sig.]
$[H(n_c, R, K_{cf}) \oplus K_{cm}]$
$[H(K_{cm}, n_c)]$
$n_{m1}, H(n_{m1}, R, K_{cm})$
$(\alpha_m{}^v \bmod \beta_m)$ & sig.
$H(n_m, R, K_{mf}) \oplus K_{cm}$
$H(K_{cm}, n_m)$
$(\alpha_c{}^u \bmod \beta_c), z$ & sig.
$H(n_c, R, K_{cf}) \oplus K_{cm}$
$H(K_{cm}, n_c)$
n_{c1}, z_c
$H(n_{c1}, z^{1/Pc}, n_{m1}, R, K_{cm})$
$[R],$
$[n_{c1}], [z_c]$
α_m, β_m
1
C
4
5
6
3
F
2
Client Protocol Unit
30
39
MD5
Controller
DSA?
38
36
P_c
$(a^{Pc} \bmod \beta_c)$
a
34
32
$(\alpha_m{}^{Pm} \bmod \beta_m)$
α_c, β_c
$(\alpha_c{}^{Pc} \bmod \beta_c)$
Financial Intermediary Protocol Unit
MD5
Controller
DSA
58
60
50
K_{cf}, K_{mf}, z
64
56
K_{cm}
$(a^b \bmod \beta_c)$
u,v,x,y
52
62

(57) Abstract

Authentication by an intermediary F (e.g. a bank) of an originator C of a message (e.g. a client sending an instruction to pay a merchant M) is accomplished using a protocol which does not require the intermediary to possess passwords used by the originator C and the merchant M to protect the contents of the message. Furthermore, the protocol does not require any party to the transaction to decrypt any value previously encrypted by any other party, so a reversible encryption algorithm is not required.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

Methods and apparatus for authenticating an originator of a message

Technical Field

This invention relates to methods and apparatus for authenticating an originator of a message, and which in particular enable the originator of a message to be authenticated without the need for specialized authentication organizations, and without decryption of encrypted information.

Background Art

Modern computing and telecommunication systems have enabled a rapid and continuing increase in exchange of information between individuals and organizations, e.g. via the system commonly known as the Internet. However, the full potential of such systems is currently restricted by the difficulty of providing secure transfer of valuable information over the system. Many organizations would like to use publically-accessible networks for conducting various transactions, such as the sale of goods and services. In principle payment for such transactions could be obtained from a customer by transfer over the network of relevant information such as credit card details. However it is clearly possible for a dishonest third party to intercept such information during transmission, and then mis-use it to the third party's financial advantage. Various other fraudulent activities are possible, such as false repudiation of orders. Accordingly most transactions which may be initiated over a network still have to be completed using conventional methods such as exchange of paper invoices and payments or voice messages, using more trusted systems such as mail or voice telephone networks.

It is essential for an effective electronic transaction mechanism to have several properties:

- authentication (i.e. confirmation of origin) of messages involved in a transaction;
- protection of the integrity of messages involved in the transaction, and ability to prove if a message has been corrupted;
- prevention of false repudiation of an agreement to make a payment;
- prevention of frauds involving recording and replaying of messages involved in a transaction;
- economy of implementation; and
- compatibility with national security interests.

Various proposals have been made for electronic message authentication. Although they tend to satisfy the primarily technical requirements, they also tend to be either costly and/or contrary to national security interests. Thus many proposals involve reliance on a specialized third-party security service, for example for authentication of messages in each transaction or to supply and certify public encryption keys. In addition many of these proposals involve the use of reversible encryption algorithms, i.e. algorithms in which information is concealed by encryption by a sender and retrieved again by decryption by the recipient. Such algorithms can also be used for transfer of other information which is contrary to national security interests, so the distribution and in particular export from some countries of products which incorporate reversible encryption algorithms is often controlled or prohibited. Any proposal which involves decryption, and thus requires a reversible encryption algorithm, is unlikely to be suitable to be made available for use on a widespread basis.

It is an object of this invention to provide a method and apparatus for authenticating messages which avoids the problems entailed in prior proposals, and in particular does not require any specialist security service nor involve the use of a reversible encryption technique.

Disclosure of Invention

According to one aspect of this invention there is provided a method for enabling authentication of an originator of a message, using a composite one-way function which enables a protected version of an input value to be derived by applying successively in either order two component one-way functions using two respective values, but which does not enable the input value to be readily determined from the protected version in combination with either of said values individually, comprising the steps of:

a) receiving a protected version of a password, said protected version being derived from a first of said component one-way functions using said password as said respective value;

b) generating another value;

c) generating a protected version of said other value by applying a second of said component one-way functions;

d) generating a digital signature for the protected version of said other value;

e) applying said second component one-way function using said other value to said protected password to derive a ticket key;

f) generating a session key;

g) protecting said session key with said ticket key;

h) supplying said protected version of said other value, said digital signature and said protected session key to the source of said protected password; and

i) thereafter destroying said other value, said ticket key and said session key.

According to one aspect of this invention there is provided apparatus for enabling authentication of an originator of a message, using a composite one-way function which enables a protected version of an input value to be derived by applying successively in either order two component one-way functions using two respective values, but which does not enable the input value to be readily determined from the protected version in combination with either of said values individually, comprising:

means for receiving a protected version of a password, said protected version being derived from a first of said component one-way functions using said password as said respective value;

means for generating another value;

means for generating a protected version of said other value by applying a second of said component one-way functions;

means for generating a digital signature for the protected version of said other value;

means for applying said second component one-way function using said other value to said protected password to derive a ticket key;

means for generating a session key;

means for protecting said session key with said ticket key;

means for supplying said protected version of said other value, said digital signature and said protected session key to the source of said protected password.

Brief Description of Drawings

Methods and apparatus for authenticating an originator of a message in accordance with this invention without the use of a reversible encryption algorithm will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 illustrates a transaction in which authentication of messages is necessary;

Figure 2 is a block schematic diagram showing the transfer of messages in a protocol by which a trusted intermediary F enables two parties C and M to authenticate each other, and verifies that C has authorized a transaction; and

Figures 3*a-c* show successive stages of the protocol.

Best Mode for Carrying Out the Invention, & Industrial Applicability

Referring to Figure 1, the invention will be described by reference to the example of a client 10 who wishes to instruct a financial intermediary 12 (such as a bank or credit card company) to make a payment to the account of a merchant 14. Each of these parties possesses a protocol unit C, F and M respectively, comprising for example appropriately-programmed computers (as in the case of the client 10 and the financial intermediary 12) or special-purpose hardware devices (as in the case of the merchant 14). These units are coupled to a communication system 16 which comprises multiple computer networks 18 interconnected by routers 20 and which typically serves many tens of thousands of users.

The networks 18 are of the kind in which at least some units attached to one network 18 can monitor messages travelling over that network between other units on the same or other networks 18. Accordingly it is not safe to transfer information such as financial transaction details in clear form over the system 16 in view of the risk of interception and misuse of that information by other parties. Furthermore, the large number of people and organizations connected to the system 16 means that for any given transaction the parties involved may never have previously had any contact. Accordingly they do not necessarily have any established relationship by means of which they might confirm each other's identity and trustworthiness. Even if such a relationship does exist there remains the risk of a fraudster masquerading as one of the parties in order to defraud the other.

The present invention provides a protocol by which the parties to a transaction, for example, can authenticate messages (i.e. confirm the origin of the messages) involved in the transaction. The method does not require the parties to share any information which one party must encode and the other must decode, for example to confirm identity; thus there is no need for a reversible encryption algorithm to be used. Although the method does entail the participation of a trusted intermediary, many existing transactions typically involve the participation of such an intermediary in the form of a financial institution, in which trust is placed, so this requirement should not normally constitute an obstacle. Furthermore the intermediary does not have to hold secret information belonging to either party.

The protocol involves the use of an arithmetic operation known as modular exponentiation, in which a first number α is raised to some power p, and this value is divided by a second number β; the desired result q is the remainder of the division operation:

$$q = \alpha^p \bmod \beta \qquad (1)$$

Modular exponentiation is a one-way function, in that although the operation of equation (1) is straightforward to perform, the inverse operation, i.e. determination of p given α, β and q, can be made extremely hard by appropriate choice of the values of α and β. β is chosen to satisfy the condition

$$\beta = 2i + 1 \qquad (2)$$

where i is a prime number. α is typically chosen to be a value which is a 'generator modulo β', meaning that the value of ($\alpha^p \bmod \beta$) varies through all values between 1 and β-1 as p varies between 1 and β-1. Pairs of values α, β can be selected so that β conforms to equation (2), for example using the method described in *Applied Cryptography* by B. Schneier, John Wiley & Sons, 1994, pp. 208-9.

Referring to Figure 2, it is first necessary for the client 10 and the merchant 14 to select respective passwords P_c and P_m, and for these to be notified in encoded form to the financial intermediary 12 once only prior to the first transaction. To this end the financial intermediary's protocol unit F selects pairs of numbers α_c, β_c and α_m, β_m as described above, stores them for future use as described below, and informs the client's protocol unit C and the merchant's protocol unit M respectively of the values of these pairs, as indicated by dashed lines 22 and 24. No particular secrecy or security is required for this step. Thus the values may be sent in printed form by mail, and entered into the protocol units via a keyboard, magnetic stripe card or the like. The client 10 selects a password (e.g. an easily memorized word, number, etc.) and enters this into the protocol unit C as well. The unit C manipulates this password in a predetermined manner to convert it to purely digital form if necessary and ensure the resulting value P_c is in one of the ranges [3, i-1] and [i+1, β_c-2], where *i* satisfies the relation $\beta_c=2i+1$, so that the value of P_c is relatively prime to β_c-1. The digital password P_c is then encoded by hashing it using equation (1) and the numbers α_c, β_c supplied by the financial intermediary 12

$$E_{P_c} = \alpha_c^{P_c} \bmod \beta_c \qquad (3)$$

If desired, to decrease vulnerability to guessing etc. of the client's selected password by another person, the digital password P_c may be concatenated with a random 'salt' value *s* before encoding, as described in *Unix operating system security* by F.T. Grampp and R.H. Morris, AT&T Bell Laboratories Technical Journal, 63, October 1984. In this case the encoding operation is

$$E_{P_c} = \alpha_c^{sP_c} \bmod \beta_c \qquad (3a)$$

The encoded value E_{P_c} is communicated to the financial intermediary 12 by the client's protocol unit C, as indicated by dashed line 26, taking reasonable precautions to verify the association of the value of E_{P_c} with the client.

In order to implement and coordinate these functions the client's protocol unit C includes a controller 30 coupled to an exponentiation unit 32, and a module 34 for deriving the digital password P_c from the client's password and for supplying it to the exponentiation unit. This unit is arranged to perform the calculation

$$a^{P_c} \bmod \beta_c \qquad (4)$$

on any value *a*, including α_c, supplied to it by the controller 30, and to furnish the result of this calculation to the controller. For security purposes the storage module 34 and the exponentiation unit 32 are designed never to output the value of the password P_c directly, as indicated schematically by the enclosure 36 around them. The values α_c, β_c and *s* (if used) may be concatenated for storage purposes to make misuse by another person of the values as stored more difficult.

The merchant likewise selects a password and enters it into the protocol unit M (for example using a smart card which is accessible to the merchant's staff). The unit M derives a corresponding digital password P_m, encodes it using the numbers α_m, β_m according to the relation

$$E_{P_m} = \alpha_m^{P_m} \bmod \beta_m \qquad (5)$$

and communicates the value E_{Pm} to the financial intermediary 12 in confidence, as indicated by the dashed line 28. The merchant's protocol unit includes a controller 40, exponentiation unit 42, storage module 44 and enclosure 46 corresponding to the items 30 to 36 in the client's unit C.

Referring to Figures 3*a* to 3*c*, in a first stage 100 of the protocol, the client 10 composes an appropriate message, such as "transfer five hundred dollars from my account no. 1234 5678 9876 to M's account no. 9876 5432 1234" and enters it into her protocol unit C. As a preliminary step to deriving a digital signature which incorporates the client's password P_c and which will accompany this message, the controller 30 in the unit 10 then generates two numbers n_c, n_{c1}; the values of these numbers may or may not be selected essentially at random (although with the restriction noted below in the case of n_{c1}), but the controller 30 is arranged to ensure that each value used is chosen afresh, for each transaction, in a manner which makes it unlikely that anyone else can predict the value chosen and unlikely that the same value will be chosen for two different transactions. As they are used on a single occasion the numbers n_c, n_{c1} are referred to as 'nonces'.

The controller 30 concatenates the nonce n_{c1} with a digital representation R of the characters comprising the client's message, and encodes the resulting sequence of digits using a one-way hashing function (such as the MD5 function described in *The MD5 message digest algorithm* by R.L. Rivest, Internet RFC 1321, April 1992) to produce a fixed-length sequence of digits represented herein as $H(n_{c1}, R)$, where H is the hashing function. The unit C includes an MD5 encoder 38 coupled to the controller 30 for effecting this hashing function. The value of n_{c1} is selected by the controller 30 so that $H(n_{c1}, R)$ is a generator modulo β_c, in the same manner as described above in respect of the number α. Selection of n_{c1} in this way makes it hard to discover the value of $H(n_{c1}, R)$ from the password-protected version (described below) which will actually be transmitted. The use of the hashing function H has the effect of compressing the size of the digital value involved, thereby facilitating subsequent calculations, and itself makes decoding computationally infeasible. The values of n_{c1} and thus of $H(n_{c1}, R)$ play a significant role in the final verification of the client's digital signature, so it is important that they are protected at this stage.

The hashed value $H(n_{c1}, R)$ is itself password-protected by the controller 30 by supplying it as the input value *a* to the exponentiation unit 32, in order to derive the client's digital signature for the message R according to the relation:

$$S_C = \{(H(n_{c1}, R))^{P_c} \bmod \beta_c\} \qquad (6)$$

The protocol unit C then sends the message R, the nonce n_c and the signature S_C to the merchant's protocol unit M through the communication system 16, as indicated in Figure 2 by the message transfer labelled 1.

In the next stage 102 (Figure 3*a*) of the protocol, the controller 40 in the protocol unit M itself selects a nonce n_m for this transaction, and forwards it to the financial intermediary's protocol unit F, together with the message R, the nonce n_c and the signature S_C received from the protocol unit C. This is indicated in Figure 2 by the message transfer labelled 2; the items R, n_c and the signature S_C are enclosed in square brackets [ ] to indicate that these values are not generated or re-calculated by the protocol unit M, but are simply forwarded as received.

When these items are received by the protocol unit F, it undertakes a series of steps comprising stage 104 (Figure 3*a*) of the protocol. To this end the protocol unit F includes a controller 50 coupled to an exponentiation unit 52 in a secure enclosure 56 in similar manner to the client's unit C. The secure enclosure 56 also contains a session key generator 60 for producing random number keys and supplying them to the controller 50; since the security of these session keys is important, the controller 50 itself is located in a secure enclosure 62. This enclosure 62 also contains an MD5 encoder 58 corresponding to the encoder 38 in the client's unit C.

The steps performed in stage 104 are as follows:

(i) Generate two nonces *u* and *v* for use once only for this purpose, in the ranges

$$[3, i\text{-}1] \text{ and } [i+1, \beta_c\text{-}2] \text{ for } u$$

$$[3, j\text{-}1] \text{ and } [j+1, \beta_m\text{-}2] \text{ for } v$$

where *i* satisfies the relation $\beta_c=2i+1$ and *j* satisfies the relation $\beta_m=2j+1$.

(ii) Compute two keys, again for use once only for the present transaction, one key K_{cf} being used by the client's unit C and the financial intermediary's unit F, and the other key K_{mf} being used by the merchant's unit M and the financial intermediary's unit F; these keys are derived by the controller 50 according to the relations:

$$K_{cf} = (E_{Pc})^u \bmod \beta_c \qquad (7)$$

$$K_{mf} = (E_{Pm})^v \bmod \beta_m \qquad (8)$$

It should be noted that the right-hand side of equation 7 can be expanded into the form

$$(\alpha_c^{Pc} \bmod \beta_c)^u \bmod \beta_c \qquad (9)$$

and that, because modular exponentiation is commutative

$$K_{cf} = (\alpha_c^{Pc} \bmod \beta_c)^u \bmod \beta_c = (\alpha_c^u \bmod \beta_c)^{Pc} \bmod \beta_c \qquad (10)$$

Thus if the client's protocol unit C is provided with the value $E_u = (\alpha_c^u \bmod \beta_c)$, which can be readily done without risking revealing the value of *u*, then the controller 30 can set *a* equal to this value E_u and compute the value of the key K_{cf} using formula (4) above. Equation (10) in effect defines a composite one-way function, comprising a first component one-way function $(\alpha_c^{Pc} \bmod \beta_c)$ using the password P_c, and a second component one-way function $((E_{Pc})^u \bmod \beta_c)$ using the value *u*. The merchant's protocol unit M can likewise compute the value of the key K_{mf} from the formula $(E_v)^{Pm} \bmod \beta_m$ where $E_v = (\alpha_m^v \bmod \beta_m)$.

(iii) Compute the values E_u and E_v, using the number pairs α_c, β_c and α_m, β_m, which the unit F originally selected, and the values *u* and *v* generated at step (i).

(iv) Obtain a random number from the session key generator 60 for use as a session key K_{cm} which will be made known to both the client's protocol unit C and the merchant's unit M, and communicated by each unit to the other to verify the sending unit's identity. To protect the session key itself, the controller 50 generates two encoding keys, one for the unit C and one for the unit M, using the hashing function provided by MD5 encoder 58, and combines the session key with these keys to produce two tickets by a bitwise exclusive-OR (XOR) operation, represented by ⊕ in the following relationships:

$$\text{ticket for C} = H(n_c, R, K_{cf}) \oplus K_{cm} \qquad (11)$$

$$\text{ticket for M} = H(n_m, R, K_{mf}) \oplus K_{cm} \qquad (12)$$

(v) To enable the integrity of these tickets to be verified by their respective recipients, generate respective verifiers $H(K_{cm}, n_c)$ and $H(K_{cm}, n_m)$, again using the hashing function provided by the MD5 encoder 58.

(vi) In preparation for verifying the client's digital signature S_C which will subsequently be forwarded by the merchant's protocol unit M, generate two more random numbers *x* and *y*, both in the ranges [3, i-1] and [i+1, β_c-2], and use them to compute a value *z* according to the relationship:

$$z = \{((S_C)^x \bmod \beta_c)((E_{Pc})^y \bmod \beta_c)\} \qquad (13)$$

(vii) Compute two digital signatures: one signature S_{FC} for the concatenation of the values E_u and *z*; and a second signature S_{FM} for the value E_v. These signatures are produced by using, for example, the Digital Signature Algorithm (DSA) defined in *Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)*, Federal Register, v. 56, no. 169, 30 Aug 1991, pp. 42980-42982, to enable the values of E_u, *z* and E_v to be authenticated upon reception. For this purpose the unit F includes a DSA encoder 64 located within the enclosure 62 and connected to the controller 50.

To conclude stage 104, the protocol unit F sends the following items back to the merchant's protocol unit M:

E_u, z and S_{FC} for the client's unit C;
E_v and S_{FM} for the merchant's unit M;
the ticket $H(n_c, R, K_{cf}) \oplus K_{cm}$ for C;
the ticket $H(n_m, R, K_{mf}) \oplus K_{cm}$ for M;
the verifiers $H(K_{cm}, n_c)$ and $H(K_{cm}, n_m)$.

This communication is indicated in Figure 2 by the message transfer labelled 3.

Upon receipt of these items the merchant's protocol unit M commences stage 106 of the protocol (Figure 3*b*). First the controller 40 in this unit checks the received value E_v by using the associated DSA signature S_{FM}; for this purpose the unit M includes a DSA verifier 49. Next the controller derives the value of the key K_{mf} using the merchant's password P_m in the formula $(E_v)^{Pm} \bmod \beta_m$. With the key K_{mf}, the digital message R received from the client C and the nonce n_m it generated at stage 102, the controller 40 can now use the MD5 encoder 48 to obtain the hashed value $H(n_m, R, K_{mf})$. By using an exclusive-OR operation of this value with the ticket $H(n_m, R, K_{mf}) \oplus K_{cm}$ defined in equation (12), the controller 40 can determine the session key K_{cm}. The integrity of this session key is verified by obtaining the hashed value $H(K_{cm}, n_m)$, using the MD5 encoder 48 again, and comparing it with the corresponding hashed value sent by the protocol unit F. The inclusion of the nonce n_m in this check confirms that the session key K_{cm} has been freshly generated.

If these checks are satisfactory, the controller 40 proceeds to generate a second nonce n_{m1} for the merchant's unit M, and then obtains a new hashed value $H(n_{m1}, R, K_{cm})$ from the MD5 encoder 48, for use in demonstrating to the client's unit C the authenticity of the next communication it receives from merchant's unit M.

For this next communication, indicated by the message transfer labelled 4 in Figure 2, the unit M sends the following items to the unit C:

E_u, z and S_{FC} (as received from the unit F);
the ticket $H(n_c, R, K_{cf}) \oplus K_{cm}$ (as received from the unit F);
the verifier $H(K_{cm}, n_c)$ (as received from the unit F);
the nonce n_{m1} and the new hashed value $H(n_{m1}, R, K_{cm})$.

In the next stage 108 of the protocol, the controller 30 in the unit C performs several steps analogous to those just performed in the unit M: it checks the received value E_u by using the associated DSA signature S_{FC}, for which purpose it includes a DSA verifier 39. Next the controller 30 derives the value of the key K_{cf} using the client's password P_c and with *a* set to the value E_u in formula (4) above. With the key K_{cf}, the digital message R and the nonce n_c it generated, the controller 30 can now use the MD5 encoder 38 to obtain the hashed value $H(n_c, R, K_{cf})$. By using an exclusive-OR operation of this value with the ticket $H(n_c, R, K_{cf}) \oplus K_{cm}$ defined in equation (11), the controller 30 can determine the session key K_{cm}. The integrity of this session key is verified by obtaining the hashed value $H(K_{cm}, n_c)$, using the MD5 encoder 38 again, and comparing it with the corresponding hashed value sent by the protocol unit F via the merchant's unit M. The inclusion of the nonce n_c in this check confirms that the session key K_{cm} has been freshly generated.

With this session key and the nonce n_{m1}, the controller 30 now obtains from the MD5 encoder 38 the hashed value $H(n_{m1}, R, K_{cm})$, and compares it with the hashed value received from the merchant's protocol unit M. If this comparison is successful, indicating that the merchant 14 is in possession of the session key K_{cm}, the authenticity of the communication from the merchant 14 has been confirmed. Accordingly the client's unit C can proceed with authorization of the transaction.

To this end, in the final part of stage 108 (Figure 3*c*), the controller 30 derives the following value to enable the financial intermediary to confirm the client's signature undeniably:

$$z_c = z^{1/P_c} \bmod \beta_c \qquad (14)$$

where $1/P_c$ indicates the inverse of the password P_c modulo (β_c-1), derived from P_c as described in *Cryptography and Data Security* by D.E. Denning, Addison-Wesley, 1982.

The controller 30 then obtains from the MD5 encoder 38 the hashed value $H(n_{c1}, z_c, n_{m1}, R, K_{cm})$ and sends it, with the value z_c and the nonce n_{c1} which was included in the digital signature S_C, to the merchant's protocol unit M, as indicated by the message transfer labelled 5 in Figure 2.

At stage 110, the controller 40 in the unit M then obtains from the MD5 encoder 48 the hashed value $H(n_{c1}, z_c, n_{m1}, R, K_{cm})$ and compares it with the value received from the unit C. If the comparison is correct, indicating that the client 10 is also in possession of the session key K_{cm} together with the message R, the authenticity of the communication from the client 10 has been confirmed. Accordingly the merchant's unit M forwards the client's confirmation of the digital signature S_C by sending the items R, n_{c1} and z_c to the protocol unit F, as indicated by the message transfer labelled 6 in Figure 2.

In the final stage 112 of the protocol, the protocol unit F, now having the nonce n_{c1}, obtains the hashed value $H(n_{c1}, R)$ from the MD5 encoder 58, and verifies the client's digital signature S_C by checking whether the following relationship is satisfied:

$$z_c = \{((H(n_{c1}, R))^x \bmod \beta_c)(\alpha_c^{\ y} \bmod \beta_c)\} \qquad (15)$$

If this relationship is satisfied, the signature is confirmed as being genuine, and cannot be repudiated (as explained below).

This protocol establishes the following facts for the financial intermediary F:

the authenticity of the client's signature;

both the client's unit C and the merchant's unit M have correctly used their keys K_{cf} and K_{mf};

both the client's unit C and the merchant's unit M have correctly used the session key K_{cm}, and they each have established that the other has correctly used it (i.e. they have each authenticated the other's identity);

these authentications relate to the message R;

by sending the nonce n_{c1} to the financial intermediary's protocol unit F, via the merchant's unit M, the client 10 has confirmed her agreement to the contents of the message R.

The protocol accomplishes these demonstrations by means of authentication performed by the trusted intermediary 12; however, it is not necessary for the intermediary F to possess the passwords P_c and P_m of the client 10 and the merchant 14: the relevant encryption is performed without the encryption function being directly available to the intermediary F. Furthermore, inspection of the protocol shows that nowhere is it necessary for any unit C, M or F to decrypt any value previously encrypted by any other unit. Thus there is no need to use a reversible encryption algorithm of a kind which would be subject to regulatory restrictions (typically an exclusive-OR operation is not regarded as falling into a restricted category).

In particular the protocol involves the use of two nonces (*u* and *v*), in a manner which does not require them to be communicated as such. Furthermore, the manner in which they are communicated (incorporated into the values E_u and E_v) does not enable them to be readily discovered, and the information they protect (K_{cf} and K_{mf}) is not communicated as such, although it can be obtained by parties properly possessing the appropriate passwords P_c and P_m without those parties needing to know the values *u* and *v* themselves. Digital signatures S_{FC} and S_{FM} are supplied with the values E_u and E_v to authenticate them, and are used for that purpose only. Accordingly, it is relatively easy and economical to implement a very secure, tamper-resistant device (i.e. the protocol unit F) to generate the one-time numbers u and v, compute the values E_u and E_v, and sign them digitally with the signatures S_{FC} and S_{FM}.

If it is necessary to prove that the digital signature S_C did originate from the client 10, this can be done by requesting the client to provide the result of the formula (4) for one hundred different numbers *a*. Ninety-nine of these numbers are chosen to have the form (α_c^x mod β_c), i.e. are derived from ninety-nine values of *x*, so the results provided by the client 10 can be checked by performing the calculation

$$((E_{Pc})^x \bmod \beta_c) \qquad (16)$$

If these ninety-nine results are correct, the client 10 is shown to have used her password P_c in obtaining them.

The remaining value *a* is derived using the formula

$$(\alpha_c^b \bmod \beta_c)(H(n_{c1}, R)) \qquad (17)$$

where *b* is selected from the ranges [3, i-1] and [i+1, β_c-2]. The result *d* provided by the client 10 from formula (4) is tested using the relationship

$$d = [S_C((E_{Pc})^b \bmod \beta_c)] \bmod \beta_c \qquad (18)$$

If this relationship is satisfied, the digital signature S_C must have been produced using the client's password P_C.

CLAIMS

1. A method for enabling authentication of an originator of a message, using a composite one-way function which enables a protected version of an input value to be derived by applying successively in either order two component one-way functions using two respective values (u, P_c), but which does not enable the input value to be readily determined from the protected version in combination with either of said values individually, comprising the steps of:

a) receiving a protected version (E_{Pc}) of a password (P_c), said protected version being derived from a first of said component one-way functions using said password (P_c) as said respective value;

b) generating another value (u);

c) generating a protected version (E_u) of said other value by applying a second of said component one-way functions;

d) generating a digital signature (S_{FC}) for the protected version (E_u) of said other value;

e) applying said second component one-way function using said other value (u) to said protected password (E_{Pc}) to derive a ticket key (K_{cf});

f) generating a session key (K_{cm});

g) protecting said session key (K_{cm}) with said ticket key (K_{cf});

h) supplying said protected version (E_u) of said other value, said digital signature (S_{FC}) and said protected session key (K_{cm}) to the source of said protected password (E_{Pc}); and

i) thereafter destroying said other value (u), said ticket key (K_{cf}) and said session key (K_{cm}).

2. The method of claim 1, wherein said component one-way functions incorporate modular exponentiation.

3. The method of claim 1 or claim 2, wherein said session key is protected with said ticket key by a bitwise exclusive-OR operation.

4. Apparatus for enabling authentication of an originator of a message, using a composite one-way function which enables a protected version of an input value to be derived by applying successively in either order two component one-way functions using two respective values (u, P_c), but which does not enable the input value to be readily determined from the protected version in combination with either of said values individually, comprising:

means for receiving a protected version (E_{Pc}) of a password (P_c), said protected version being derived from a first of said component one-way functions using said password (P_c) as said respective value;

means for generating another value (u);

means for generating a protected version (E_u) of said other value by applying a second of said component one-way functions;

means for generating a digital signature (S_{FC}) for the protected version (E_u) of said other value;

means for applying said second component one-way function using said other value (u) to said protected password (E_{Pc}) to derive a ticket key (K_{cf});

means for generating a session key (K_{cm});

means for protecting said session key (K_{cm}) with said ticket key (K_{cf});

means for supplying said protected version (E_u) of said other value, said digital signature (S_{FC}) and said protected session key (K_{cm}) to the source of said protected password (E_{Pc}).

1/5

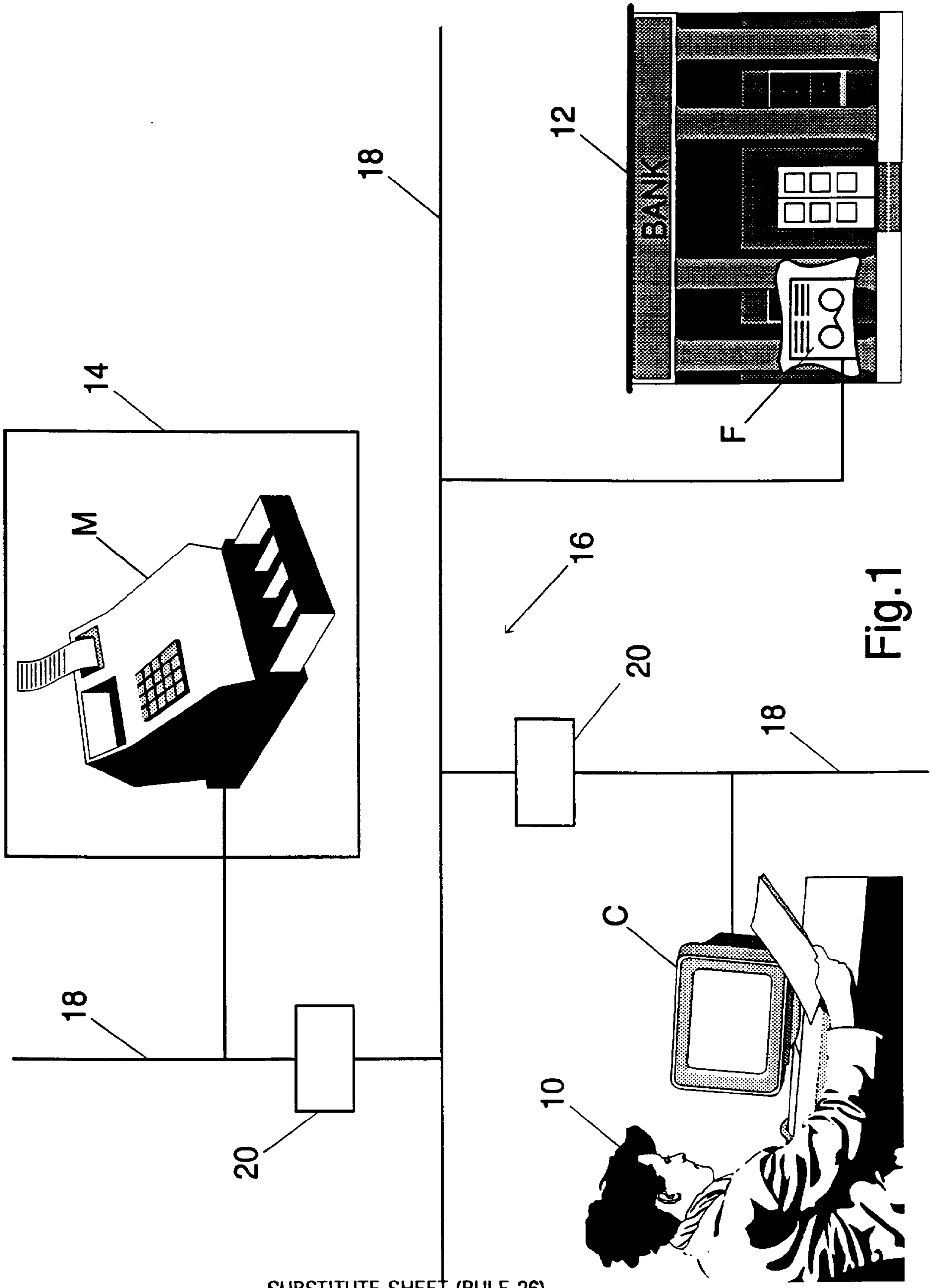


Fig.1

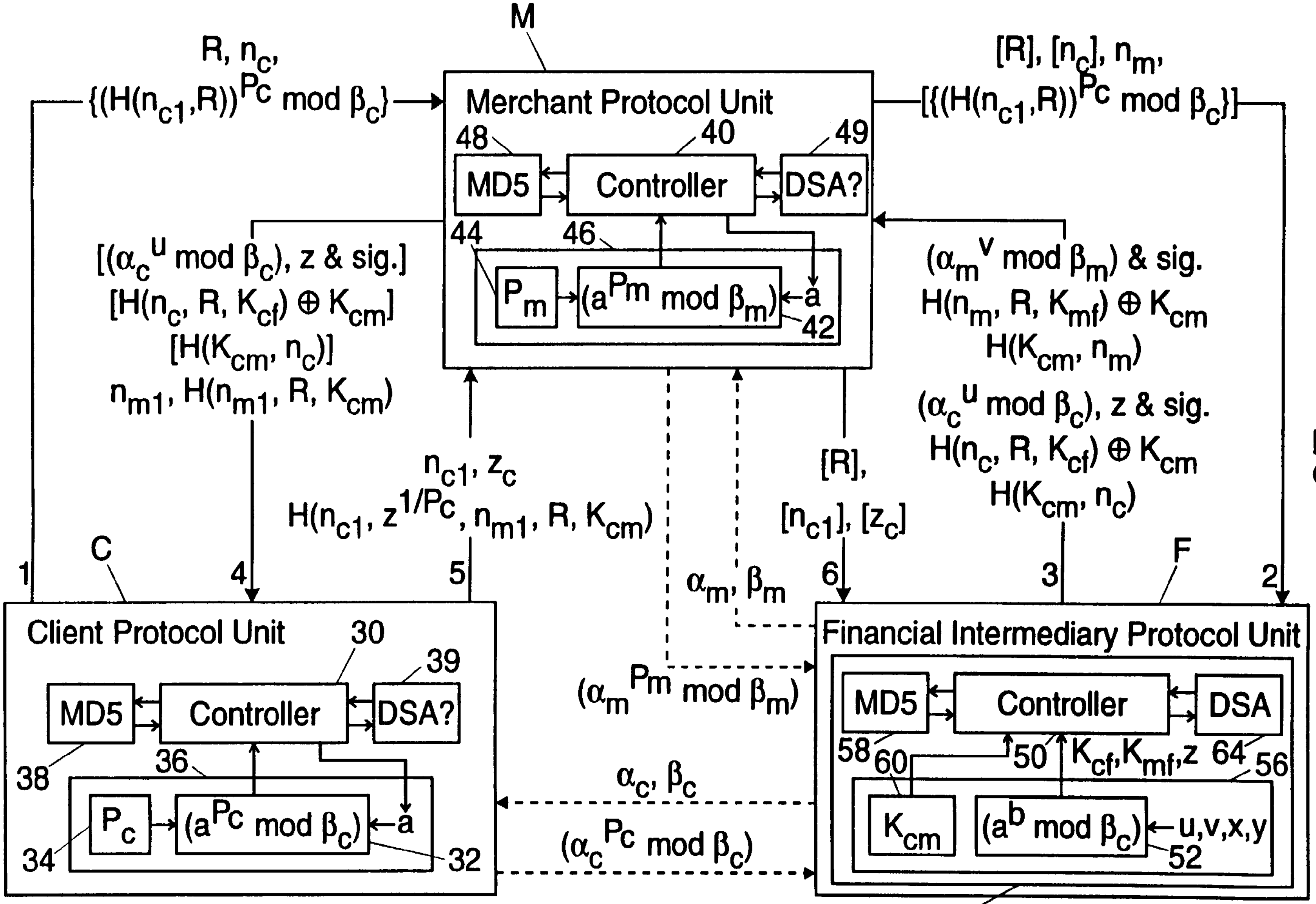

M
Merchant Protocol Unit
48
40
49
MD5
Controller
DSA?
44
46
P_m
$(a^{P_m} \bmod \beta_m)$
a
42
R, n_c,
$\{(H(n_{c1},R))^{P_c} \bmod \beta_c\}$
[R], $[n_c]$, n_m,
$[\{(H(n_{c1},R))^{P_c} \bmod \beta_c\}]$
$[(\alpha_c{}^u \bmod \beta_c)$, z & sig.]
$[H(n_c, R, K_{cf}) \oplus K_{cm}]$
$[H(K_{cm}, n_c)]$
n_{m1}, $H(n_{m1}, R, K_{cm})$
$(\alpha_m{}^v \bmod \beta_m)$ & sig.
$H(n_m, R, K_{mf}) \oplus K_{cm}$
$H(K_{cm}, n_m)$
$(\alpha_c{}^u \bmod \beta_c)$, z & sig.
$H(n_c, R, K_{cf}) \oplus K_{cm}$
$H(K_{cm}, n_c)$
n_{c1}, z_c
$H(n_{c1}, z^{1/P_c}, n_{m1}, R, K_{cm})$
[R],
$[n_{c1}]$, $[z_c]$
α_m, β_m
$(\alpha_m{}^{P_m} \bmod \beta_m)$
α_c, β_c
$(\alpha_c{}^{P_c} \bmod \beta_c)$
1
4
5
6
3
2
C
Client Protocol Unit
30
39
MD5
Controller
DSA?
38
36
P_c
$(a^{P_c} \bmod \beta_c)$
a
34
32
F
Financial Intermediary Protocol Unit
MD5
Controller
DSA
58
60
50
K_{cf},K_{mf},z
64
56
K_{cm}
$(a^b \bmod \beta_c)$
u,v,x,y
52
62

Fig.2

Fig.3a

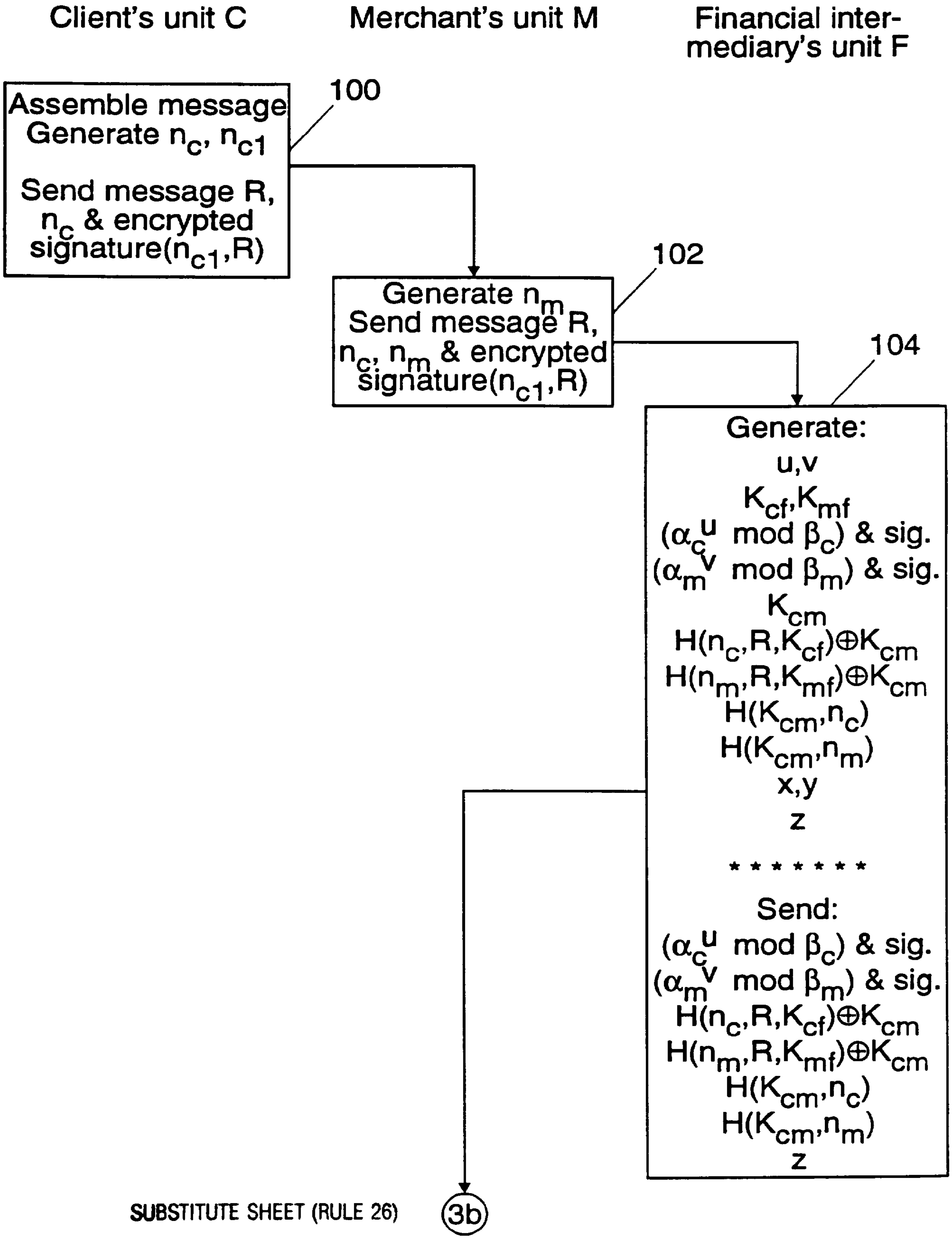

Client's unit C
Merchant's unit M
Financial intermediary's unit F
100
Assemble message
Generate n_c, n_{c1}
Send message R, n_c & encrypted signature(n_{c1},R)
102
Generate n_m
Send message R, n_c, n_m & encrypted signature(n_{c1},R)
104
Generate:
u,v
K_{cf},K_{mf}
(α_c^u mod β_c) & sig.
(α_m^v mod β_m) & sig.
K_{cm}
$H(n_c,R,K_{cf})\oplus K_{cm}$
$H(n_m,R,K_{mf})\oplus K_{cm}$
$H(K_{cm},n_c)$
$H(K_{cm},n_m)$
x,y
z
* * * * * * *
Send:
(α_c^u mod β_c) & sig.
(α_m^v mod β_m) & sig.
$H(n_c,R,K_{cf})\oplus K_{cm}$
$H(n_m,R,K_{mf})\oplus K_{cm}$
$H(K_{cm},n_c)$
$H(K_{cm},n_m)$
z
3b

Fig.3b

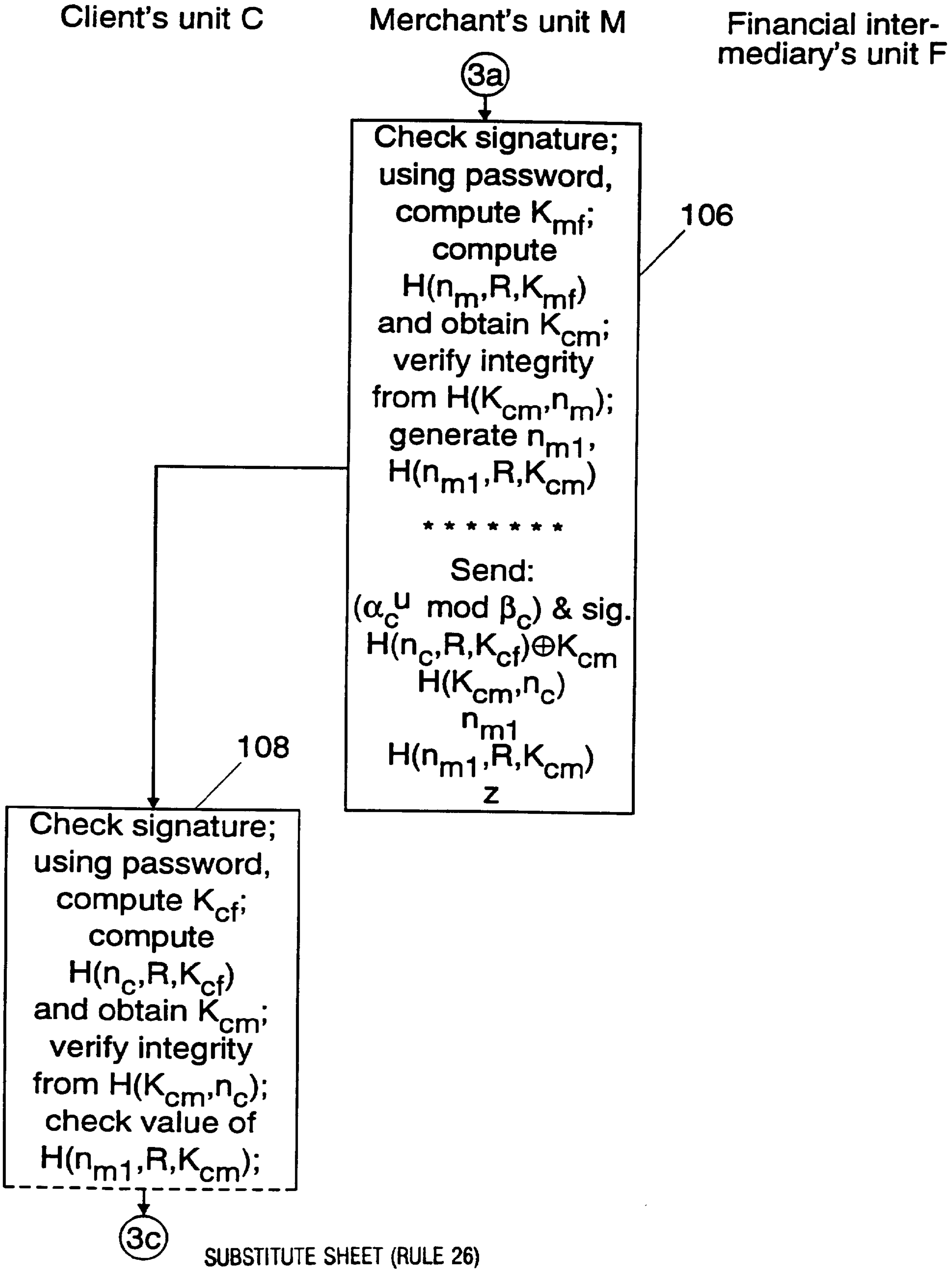
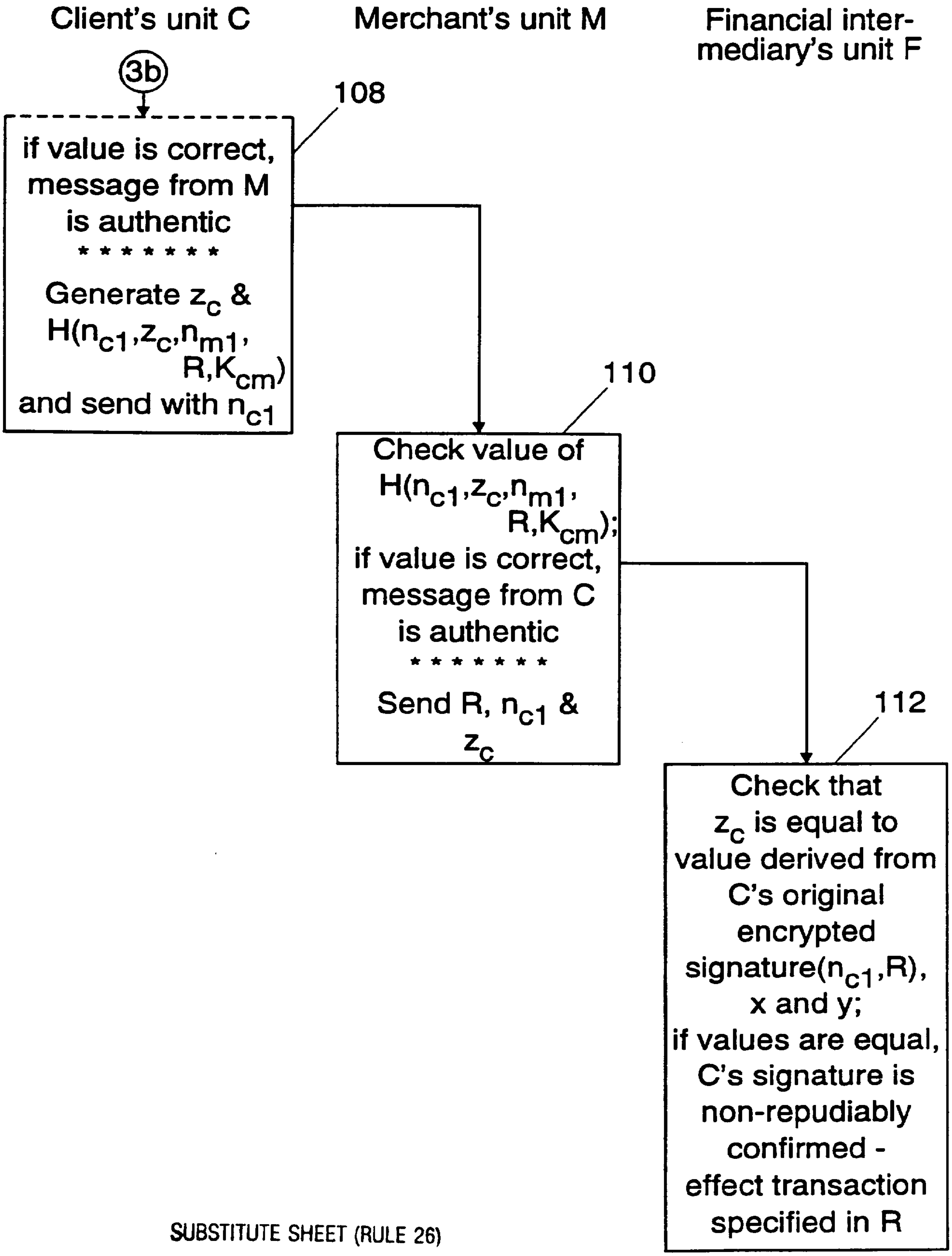

Client's unit C
Merchant's unit M
Financial intermediary's unit F
3a
Check signature; using password, compute K_{mf}; compute $H(n_m,R,K_{mf})$ and obtain K_{cm}; verify integrity from $H(K_{cm},n_m)$; generate n_{m1}, $H(n_{m1},R,K_{cm})$
* * * * * * *
Send: $(\alpha_c^u \bmod \beta_c)$ & sig. $H(n_c,R,K_{cf}) \oplus K_{cm}$ $H(K_{cm},n_c)$ n_{m1} $H(n_{m1},R,K_{cm})$ z
106
108
Check signature; using password, compute K_{cf}; compute $H(n_c,R,K_{cf})$ and obtain K_{cm}; verify integrity from $H(K_{cm},n_c)$; check value of $H(n_{m1},R,K_{cm})$;
3c

Fig.3c


Client's unit C
Merchant's unit M
Financial intermediary's unit F
3b
108
if value is correct, message from M is authentic
* * * * * * *
Generate z_c & $H(n_{c1}, z_c, n_{m1}, R, K_{cm})$ and send with n_{c1}
110
Check value of $H(n_{c1}, z_c, n_{m1}, R, K_{cm})$; if value is correct, message from C is authentic
* * * * * * *
Send R, n_{c1} & z_c
112
Check that z_c is equal to value derived from C's original encrypted signature(n_{c1},R), x and y; if values are equal, C's signature is non-repudiably confirmed - effect transaction specified in R

INTERNATIONAL SEARCH REPORT

Intern ıal Application No
PCT/GB 96/00915

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO,A,91 14980 (SIEMENS NIXDORF) 3 October 1991 see page 5, line 22 - line 31 see page 6, line 5 - line 16 see page 6, line 30 - line 32 see page 8, last paragraph - page 9, line 21 see page 10, line 3 - page 11, line 12 see page 14, paragraph 1 ---	1,2,4
A	OPERATING SYSTEMS REVIEW, JAN. 1987, USA, vol. 21, no. 1, ISSN 0163-5980, pages 8-10, XP002008756 OTWAY D ET AL: "Efficient and timely mutual authentication" see page 9, left-hand column, line 1 - page 10, left-hand column, last line -----	1,4

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search 18 July 1996	Date of mailing of the international search report 12.08.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Authorized officer Holper, G

INTERNATIONAL SEARCH REPORT

.ormation on patent family members

Interr nal Application No
PCT/GB 96/00915

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-9114980	03-10-91	DE-A-	4008971	26-09-91
		EP-A-	0472714	04-03-92
		JP-T-	4504020	16-07-92
		US-A-	5323146	21-06-94